Chapter 12
3D/2.5D IC-Based Obfuscation

Yang Xie, Chongxi Bao and Ankur Srivastava

12.1 Introduction

Physical limit of transistor miniaturization has driven chip design into the third dimension. 3D integration technology emerges as a viable option to improve chip performance in a direction orthogonal to costly device scaling [10]. A typical stacked 3D IC structure is illustrated in Fig. 12.1a. It expands the circuit design space by vertically stacking multiple device layers and interconnecting them using vertical connections called Through-Silicon-Vias (TSVs). This emerging technology improves chip performance in various aspects. The vertical stacking structure is an attractive option for increasing transistor density. It breaks new ground in system-level integration by integrating more devices and resources into one chip. Besides, 3D integration reduces interconnect wirelength because two distant devices in a conventional 2D design can be placed vertically close to each other and connected with a shorter connection in 3D ICs. The reduction in wirelength scales down interconnect power and delay, which can be leveraged by implementing a more highly connected architecture such as the high-bandwidth Memory-on-Chip architecture [10]. Moreover, 3D integration allows heterogeneous integration. Separate layers can be fabricated using disparate materials and technologies. Heterogeneous integration optimizes existing System-on-Chip (SoC) designs by integrating components of different novel technologies into a single chip. Another structure of 3D IC is called interposer-based 3D IC (or 2.5D IC), as shown in Fig. 12.1b. In this structure, multiple dies are placed side-by-side on a silicon interposer, which provides chip-scale interconnections

Y. Xie (✉) · C. Bao · A. Srivastava
University of Maryland, College Park, MD 20742, USA
e-mail: yangxie@umd.edu

C. Bao
e-mail: borisbcx@umd.edu

A. Srivastava
e-mail: ankurs@umd.edu

D. Forte et al. (eds.), *Hardware Protection through Obfuscation*,
DOI 10.1007/978-3-319-49019-9_12

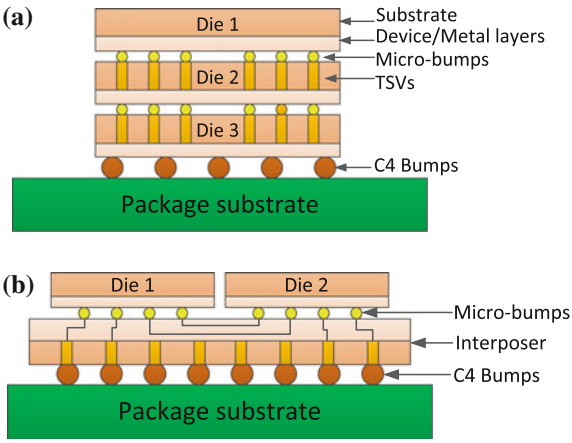

Fig. 12.1 Two common structures of 3D ICs: **a** Stacked 3D IC and **b** Interposer-based 3D IC (2.5D IC)

among different dies. 2.5D integration offers a better thermal cooling option than stacked 3D ICs while still enjoys comparable performance benefits, hence it is viewed as a step stone to stacked 3D integration.

As 3D/2.5D integration is becoming a promising technology for next-generation chip design, researchers have started to investigate it from a hardware security perspective [46]. One line of research focuses on utilizing 3D/2.5D IC technology to protect IC designs from being pirated or tampered during outsourced fabrication [4, 15, 26, 38, 45, 47]. Nowadays, IC designs are increasingly outsourced to an offshore fabrication foundry due to the increasing complexity of modern IC designs and the huge capital expenditure for developing an advanced semiconductor foundry [11]. This poses new security threats on the outsourced designs since the offshore foundry might not be trustworthy. Potential attacks include intellectual property (IP) piracy, overproduction, and malicious modification (hardware Trojans), as discussed in previous chapters. With 3D/2.5D integration, a designer can choose a portion of layers at his discretion and fabricate them in a trusted foundry while outsourcing the rest to untrusted foundries for advanced fabrication technology. This split fabrication strategy of 3D/2.5D ICs creates a new opportunity to obfuscate the outsourced designs. Without the knowledge of the layers that are fabricated in the trusted foundry, an attacker in the untrusted foundry can only observe an incomplete netlist that is a part of an original design. Therefore, it is difficult for him to pirate or counterfeit the complete design, or insert hardware Trojans at a targeted place. 3D/2.5D-based obfuscation enables the access of offshore semiconductor foundries while reducing the security threats in outsourced fabrication.

3D/2.5D integration not only boosts chip performance, but also unlocks new opportunities to thwart security threats in a global IC supply chain. At the same time, it also brings new design and security challenges. This chapter presents the current state of 3D/2.5D IC-based obfuscation techniques and highlights potential security opportunities and challenges of this technology in hardware intellectual property (IP) protection. The outline of this chapter is as follows. Section 12.2 gives an overview of

3D/2.5D integration technology. Section 12.3 discusses 3D/2.5D IC-based obfuscation enabled by 3D/2.5D split fabrication strategy. Section 12.4 summarizes different design objectives, metrics and granularities of 3D/2.5D split fabrication. Section 12.5 introduces a security-aware 2.5D IC design flow that aims at thwarting hardware IP piracy. Section 12.6 discusses various security challenges in 3D/2.5D ICs. Finally, Sect. 12.7 summarizes the implications of 3D/2.5D-based obfuscation on the design of computer-aided design (CAD) tool and Sect. 12.8 concludes this chapter.

12.2 3D/2.5D Integration Technology

3D integration is a technology that vertically integrates multiple 2D dies to create a single high-performance chip, referred to as 3D IC. In general, 3D ICs can be fabricated in two ways. Conventional *die-stacking-based 3D fabrication* utilizes existing 2D IC fabrication process to fabricate multiple 2D dies separately on different substrates and then stack them vertically. Vertical interconnects between different layers are enabled by TSVs. TSVs are vertical electrical connections which are typically made of copper or tungsten. They penetrate through a silicon substrate to connect device layers of different dies, as shown in Fig. 12.1a. TSVs are essential components in die-stacking-based 3D ICs because they provide inter-layer signal communication, thermal conducting and power delivery. Another emerging 3D IC fabrication technology is *monolithic 3D fabrication* [5]. Unlike die-stacking-based 3D fabrication, it grows multiple device layers vertically on the same substrate in a serial order, so it does not require die alignment and bonding while die-stacking-based 3D fabrication does. Because die-stacking-based 3D fabrication has received more attention from both academia and industry due to its fabrication compatibility, we focus on this technique in the following discussion.

Two common structures of 3D ICs are stacked: 3D IC and interposer-based 3D IC (also known as 2.5D IC). Figure 12.1a illustrates the structure of a stacked 3D IC. Multiple TSV-penetrated dies are stacked and bonded vertically. The stacking structure offers various performance advantages as discussed in Sect. 12.1. However, the increased device density in stacked 3D ICs brings about thermal, power and reliability issues. To alleviate these issues while still enjoying the performance benefit, 2.5D IC has been proposed (as shown in Fig. 12.1b). Unlike stacked 3D ICs, 2.5D IC places multiple dies side-by-side and bonds them on a silicon interposer through fine-pitch micro-bumps. The interposer contains both horizontal chip-scale interconnect wires between dies as well as vertical interconnect TSVs to external I/O pins. However, TSVs are not required for inter-die communication in 2.5D ICs. The absence of TSVs in the dies of 2.5D IC makes it easier to design and fabricate than TSV-penetrated stacked 3D IC. Although 2.5D ICs might not achieve the same amount of performance improvement as 3D ICs, it offers better cooling options, which is essential for high-performance computing systems. While commercial large scale 3D IC is still being developed, large-volume commercial 2.5D products are already in the market, such as the Xilinx Virtex-7 2000T FPGA [34].

3D integration can be done at different granularities [22]. Coarse-grained 3D integration can be implemented at *core level*, such as the 3D memory-on-chip architectures. This approach could offer significant improvements to performance and power and alleviate the memory bandwidth wall problem, a situation in which the chip-to-memory bandwidth is becoming a performance and throughput bottleneck. But the core-level integration does not take full advantage of the benefits of 3D ICs. A finer grained *functional block level* integration allows functional blocks to be distributed across multiple layers but maintain each functional block as a 2D circuit. This can reduce intra-core wirelength and allow reduced clock period or power. To take this idea even further, 3D integration at the *logic-gate level* offers even more savings in power and delay. It implements an individual functional block across multiple layers so as to reduce intra-block delays and power. A recent study [17] of full-chip 3D design of a SPARC chip multiprocessors (CMP) showed that a 3D design using 2D functional blocks can reduce power by 14% compared to a baseline 2D design, however when the logic-gate level 3D integration is applied this reduction in power becomes 20%. Even finer grained integration at the *transistor level* (e.g. separate layer for NMOS and PMOS) has been considered [22], but the ability to manufacture TSVs at the size and pitch required for such a scheme is yet to be realized. Moreover, the reliability and yield implications of such an approach are expected to be prohibitive [23].

12.3 3D/2.5D IC-Based Obfuscation

As 3D/2.5D integration is becoming a promising technology for next-generation chip design, researchers have started to investigate it from a hardware security perspective. One line of research focuses on utilizing 3D/2.5D ICs to mitigate security threats in outsourced fabrication [4, 15, 26, 38, 45, 47]. In order to access advanced semiconductor technology at a lower cost, most IC design companies that once possessed their own foundries are now adopting a fabless model: they concentrate their resources and efforts on IC designs while outsourcing the fabrication. Although such outsourcing model is cost-effective, it poses new security threats on the outsourced designs since the offshore foundry might not be trustworthy. Without close monitoring and direct control, the outsourced designs are vulnerable to various attacks such as piracy, overproduction and hardware Trojan insertion, as discussed in previous chapters. These attacks (also known as supply chain attacks) pose not only an economic risk to commercial IC design companies, but also security threats for sensitive electronic systems. In this section, we discuss how to utilize 3D/2.5D integration to mitigate these attacks.

12.3.1 3D/2.5D Split Fabrication

In 3D/2.5D integration, multiple dies (active layers) are fabricated independently on separate substrates and then integrated together into a single chip. This fabrication process offers inherent support for *split fabrication*, where different dies can be fabricated in different foundries. A designer can choose a portion of the design at his discretion and manufacture it in a trusted foundry for security while manufacturing the rest in an untrusted foundry for state-of-the-art fabrication technology. Because a portion of the original design will be hidden from the untrusted foundry, *3D/2.5D split fabrication* creates a new opportunity to access offshore fabrication foundries while preventing potential security threats.

3D split fabrication can take place in two different forms [38, 42]. In one embodiment, some dies (active layers) of a stacked 3D IC are fabricated in a trusted foundry, referred to as *trusted tier* while others are outsourced to one or more untrusted foundries, referred to as *untrusted tier*, as shown in Fig. 12.2a. The final integration is also implemented in the trusted foundry. With that, each untrusted foundry can only obtain one portion of design and thus it is difficult to reverse-engineer the original design or insert hardware Trojans at a desired place. Even if we assume all untrusted foundries are colluded (as one untrusted foundry), the portion of IC design in the trusted tier is not directly accessible to the untrusted foundries and hence it is protected from potential attacks by the adversary. In another embodiment, all active layers are outsourced to the offshore foundries and then securely routed and bonded in a trusted foundry. By doing so, the vertical connections between layers are kept secret. Although the offshore foundries can reverse-engineer the netlist of each layer, the resultant incomplete netlist (lacking the inter-layer connections) is incomprehensible if a design is intelligently partitioned into different layers in an obfuscated manner.

For 2.5D split fabrication [15, 45, 47], the most common split fabrication strategy is to fabricate the silicon interposer in a trusted foundry as the trusted tier while

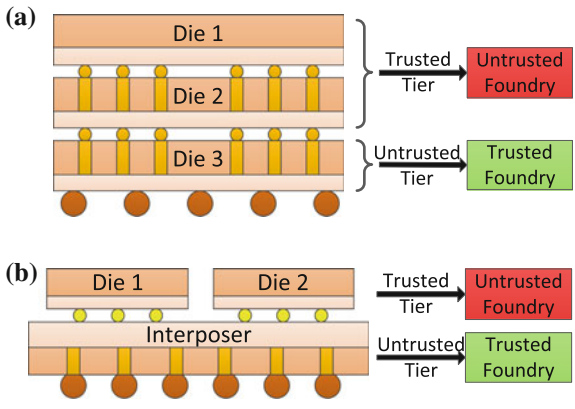

Fig. 12.2 3D split fabrication for **a** stacked 3D IC and **b** 2.5D IC

outsourcing the dies as the untrusted tier, as shown in Fig. 12.2b. If all untrusted foundries are independent (not colluded), an attacker in one untrusted foundry can only obtain the netlist of a die that is fabricated in this foundry. Even if the offshore foundries are colluded, they can at most obtain an incomplete design that lacks these interconnect wires. The incomplete netlist will be incomprehensible if the wires in the interposer layer are intelligently selected. As discussed in Sect. 12.2, 2.5D integration has less severe thermal and reliability challenges while offering a comparable performance improvement compared to the stacked 3D integration. Moreover, leveraging this technology requires only minor modification to current IC design flow and fabrication process. As a result, recent research work on 3D IC-based obfuscation [15, 45, 47] focuses more on 2.5D split fabrication than stacked 3D IC-based split fabrication.

12.3.2 Comparison Between 3D/2.5D and 2D Split Fabrication

Notice that the split fabrication strategy can also be applied to conventional 2D IC technology [16, 29, 40, 41]. As shown in Fig. 12.3, 2D IC-based split fabrication (also known as *split manufacturing*) splits a 2D IC into a Front-End-Of-Line layer (FEOL) that contains active devices and lower metal layers, and a Back-End-Of-Line (BEOL) layer that contains higher metal layers. The FEOL layer is outsourced to an untrusted foundry for advanced fabrication technology while the fabrication of BEOL layer and final integration are securely implemented in a trusted foundry. Thus, interconnect wires in BEOL layer of a split 2D IC are kept secret from the untrusted foundry.

Compared to 2D split fabrication, 3D/2.5D split fabrication requires less strict fabrication compatibility between the untrusted foundry and the trusted foundry and can provide more flexibility on obfuscation design. The difference between 2D and 3D/2.5D split fabrication are summarized as follows.

- *Alignment and integration*: for a split 2D IC, the alignment and integration are more challenging especially when the 2D IC is split from a low metal layer [45]. In general, a low-layer split 2D IC has smaller pitch length (eg 0.1–1.6 μm [45]) and

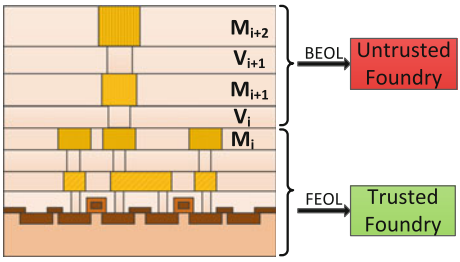

Fig. 12.3 2D split fabrication. A 2D IC is split into a FEOL layer that contains active devices and lower metal layers, and a BEOL layer that contains higher metal layers

dense connections across trusted BEOL and untrusted FEOL layer, which requires more precise alignment and integration techniques. In contrast, the alignment of TSVs of 3D/2.5D IC is less challenging because of larger pitch size (eg 5 μm [24]) and less number of connections.

- *Fabrication process*: the split fabrication strategy of 3D/2.5D IC is adaptable to off-the-shelf 3D/2.5D IC fabrication process. Each die is an individual component that can be fabricated separately and then integrated together, either in a single foundry or in different foundries. Interconnecting separately made dies using 3D integration is already a proven technology [42]. Thus, the extra effort for 3D/2.5D IC to adapt the split fabrication is lower than that of 2D IC.
- *Obfuscation flexibility*: in terms of obfuscation, the trusted tier of 3D IC consists of active layers which can be used to hide logical gates and functional circuits while for 2D ICs, the trusted BEOL layer is restricted to be metal wires. As a result, the complexity for an adversary to reconstruct the whole design for 3D/2.5D split fabrication is much higher than 2D split fabrication [20].

12.3.3 Comparison Between 3D/2.5D Split Fabrication and Logic Locking

Logic locking [3, 18, 21, 27, 28, 31, 33, 43] is another hardware IP protection technique that hides the functionality of an IC by inserting additional key-controlled logic gates (eg XOR/XNOR) and key-inputs into a circuit, as introduced in previous chapter. The locked circuit preserves the correct functionality only when the key-inputs are set correctly. Although both logic locking and 3D/2.5D split fabrication aim at obfuscating the outsourced design to prevent security threats in outsourced fabrication, these two techniques differ in various aspects:

- *Obfuscation Approach*: Obfuscation by logic locking is implemented by "adding" extra logic gates to make the original circuit become a key-controlled reconfigurable circuit. On the contrary, 3D/2.5D split fabrication is implemented by "subtracting" a portion of gates/wires and hiding them in the trusted tier so as to prevent the complete exposure of the original design.
- *Attack Resistance*: 3D/2.5D split fabrication is believed to be more attack-resistant than logic locking [20]. For logic locking, although the outsourced design is locked with additional key-gates, its layout and hence netlist are completely exposed to the untrusted foundry. Once the correct key is known, the correct functionality and netlist are accessible to an attacker. Various attacks have been proposed to infer the correct key of logic locking techniques [27, 28, 36, 48]. On the contrary, 3D/2.5D split fabrication hides a portion of design in the trusted tier, so the untrusted foundry does not have access to the complete netlist. The trusted tier behaves as a black box and thus it is more difficult for an adversary to infer the functionality of the trusted tier.

- *Fabrication Compatibility*: 3D/2.5D split fabrication requires the usage of emerging 3D/2.5D integration technology while logic locking can utilize existing well-developed 2D IC technology.

12.4 Design of 3D/2.5D Split Fabrication

3D/2.5D IC technology offers a new opportunity to obfuscate the outsourced IC designs by hiding partial circuitry into a trusted tier that's fabricated in a trusted foundry. To fully exploit this idea, one important challenge is to determine the portion of circuit design that needs to be hidden and protected in the trusted tier. In this section, we introduce different design objectives, metrics and granularities for 3D/2.5D split fabrication.

12.4.1 Design Objectives and Metrics

12.4.1.1 Functionality Obfuscation

Functionality obfuscation by 3D/2.5D split fabrication aims at obfuscating the functionality of an outsourced design (the untrusted tier). It hides gates/wires into the trusted tier such that the functionality of the untrusted tier (or a *reconstructed circuit* that is inferred based on the untrusted tier) differs substantially from the original functionality. By obfuscating the functionality, an attacker who has the knowledge of the untrusted tier cannot infer or utilize the functionality of the original complete design, thereby protecting the outsourced design from piracy and overproduction.

Hamming distance (HD) is widely used to quantify the security level of functionality obfuscation [29, 30, 32, 47]. It is defined as the number of different output bits between original netlist and reconstructed netlist on applying a same input vector. Given one input vector $\mathbf{X_i}$, the function of original netlist F will produce an output vector $\mathbf{Y_i} = F(\mathbf{X_i})$, while the function of reconstructed netlist $F^{'}$ will produce another output vector $\mathbf{Y_i}^{'} = F^{'}(\mathbf{X_i})$, the HD between two outputs $HD(\mathbf{Y}_i^{'}, \mathbf{Y}_i)$ is the number of different bits in two output vectors, and the normalized HD of two functions can be calculated as follows:

$$HD(F, F^{'}) = \frac{1}{n}\sum_{i=1}^{n}\frac{HD(\mathbf{Y}_i^{'}, \mathbf{Y}_i)}{|\mathbf{y}|} \times 100\% \tag{12.1}$$

where n is the number of input vectors and $|\mathbf{Y}|$ is the number of output bits. Since the objective of functionality obfuscation is to restrain the attacker's ability to infer or utilize the correct functionality, HD approaching 50% is desirable, which indicates that the functionality of the reconstructed netlist deviates substantially away from the original functionality.

12.4.1.2 Netlist Obfuscation

Netlist obfuscation by 3D/2.5D split fabrication aims at obfuscating the netlist structure of the untrusted tier (eg the connection degree of each gates and the gate types) so that an attacker is not capable of identifying a desired place to insert hardware Trojans in the untrusted tier. These hardware Trojans are referred to as *targeted hardware Trojans*, because they aim at modifying specific targeted gates/wires to achieve some purposeful attacks such as privilege level escalation [15] or tampering hardware Trojan detection circuitries [26, 45]. By hiding enough gates/wires into the trusted tier, a targeted circuitry is partially (or completely) hidden in the trusted tier, thereby preventing the attacker for identifying the target gates/wires to attack.

Imerson et al. [15] proposed a security metric called *k-security* for evaluating the netlist obfuscation level of a 2.5D split fabrication design under targeted hardware Trojan insertion. An incomplete netlist in the untrusted tier is said to be k-secure if every gate in the original netlist can be mapped to at least k indistinguishable gates in the incomplete netlist. The k-security ensures that an attacker cannot find out the targeted gate out of the k indistinguishable gates to attack. As a result, he can either insert Trojans at one gate but has only $1/k$ success probability, or he can attack all k gates but at the risk of being detected since he needs to modify more gates.

12.4.1.3 Layout Obfuscation

The security of 3D/2.5D split fabrication rests upon the assumption that the attacker does not know the hidden portion (trusted tier) and cannot infer it based on the exposed portion of design (untrusted tier). Otherwise, the attacker can reconstruct the complete design and continue to conduct the supply chain attacks. For example, Rajendran et al. [29] proposed an attack called *proximity attack* that can be utilized to infer the hidden connection in 2.5D split fabrication. In a split-fabricated 2.5D IC, a portion of wires are hidden in the trusted tier (interposer), and they are not accessible to the untrusted foundry. However, modern floor planning and placement (F&P) tool will place two connected pins closely in the untrusted tier so as to reduce the wirelength, thereby leaking the information of the hidden connections. Since the layout information for each die is known to the attacker, he can iteratively connect an output pin in one die to its closet input pin in other die and thus reconstruct the circuit. Therefore, it is of great significance to obfuscate the layout (by placing two connected pins far away) in order to prevent the leakage of the trusted tier, especially in the case of 2.5D split fabrication.

Proximity-attack correctness is a security metric that is used to quantify the layout obfuscation level under the proximity attack. For 2.5D split fabrication, it is defined as the percentage of correct connections that are recovered by the proximity-attack algorithm. Attack correctness approaching 0% is desirable for a secure layout design, which indicates that the attacker cannot infer the correct connections in the trusted tier of a split 2.5D design.

12.4.1.4 Trusted Tier Protection

In Sect. 12.4.1.3, we introduce the proximity attack that utilizes the layout information of the trusted tier to infer the connections in the untrusted tier of a 2.5D IC. Another potential attack to infer the trusted tier can be implemented by reverse-engineering the final product obtained from the open market. The attacker can purchase the IC from the open market and utilize state-of-the-art reverse-engineering technique [39] to obtain the design of the trusted tier by delayering and extracting the chip. Therefore, tamper-resistant techniques should be applied to protect the trusted tier.

The percentage of gates correctly extracted from a layout is one of the security metrics for IC reverse-engineering [32, 39]. Thus, the security metric for trusted tier protection against reverse-engineering can be defined as the percentage of gates/wires extracted from the layout of the trusted tier, referred to as the *reverse-engineering correctness*.

12.4.1.5 Performance and Fabrication Cost

Noticing that usually the untrusted offshore foundries support more advanced technology nodes and operate at a lower cost than the trusted foundries, the choice of which part to hide is actually a trade-off among security, performance and fabrication cost. If more gates/wires need to be fabricated in the trusted foundry, the overall fabrication cost will be increased (if same technology is used). If a less advanced semiconductor technology is used for the trusted tier to reduce cost, the performance of the overall circuit will be compromised.

Area, wirelength, delay and *power* are widely used to quantify the performance of an IC design. In summary, the objective of a secure 3D/2.5D split fabrication design is to increase the circuit obfuscation level and prevent the leakage of the trusted layer at an acceptable performance/fabrication cost. The summary of design objectives and metrics is shown in Table 12.1.

Table 12.1 Design objectives and metrics for 3D/2.5D split fabrication

Design objectives	Metrics
Functionality obfuscation	HD [29, 47]
Netlist obfuscation	k-security [15]
Layout obfuscation	Proximity-attack correctness [29, 47]
Trusted tier protection	Reverse-engineering correctness [32, 39]
Performance	Area, wirelength, delay, power [15, 29, 47]

12.4.2 Design Granularities

3D/2.5D split fabrication can be designed at different granularities.

At *block-level*, the trusted tier can conceal the whole security-critical circuit blocks such as hardware Trojan detection sensors in order to protect them from being tampered or removed by the attacker. Recent years have seen a huge proliferation of hardware Trojan detection research based on functionality verification [35], side-channel signatures [2], built-in self-authentication (BISA) [44] and so on. Most of these techniques require additional circuits to assist in Trojan activation and/or detection, including dummy flip-flops, sensors and authentication circuits, which are referred to as design-for-security (DfS) circuitries. However, these DfS circuitries may also be tampered or bypassed, which undermines the system's security. With 3D/2.5D split fabrication, the DfS circuitries can be placed in the trusted tier, thereby preventing them from being identified and tampered.

At *gate-level*, the trusted tier can withhold a portion of original wires and/or gates that can maximally obfuscate the functionality and/or netlist of the exposed untrusted tier in order to prevent piracy or targeted hardware Trojan, as discussed in Sects. 12.4.1.1 and 12.4.1.2.

With technology progresses, future 3D/2.5D split fabrication might be implemented at *transistor level*. Although such fine-grained integration has not yet been realized, it offers a novel opportunity for obfuscating a lower-level component such as standard cells.

12.5 Security-Aware 2.5D IC Design Flow Against IP Piracy

Due to the advantages in thermal cooling and fabrication compatibility, 2.5D-based obfuscation has been investigated more in recent research work [15, 45, 47] compared to 3D-based obfuscation. By fabricating the interposer of 2.5D IC in a trusted foundry while outsourcing the rest to an untrusted foundry, an attacker in the untrusted foundry can only obtain an incomplete netlist which lacks the wires in the trusted tier (interposer). However, this does not imply that a conventional performance-driven 2.5D IC design flow followed by a split fabrication strategy is security optimal. In a performance-driven 2.5D IC design flow, a netlist is first partitioned in a way that minimizes the number of cut-wires to reduce the number of wires that need to be routed in the trusted tier. Then, corresponding layouts are generated using placement and routing tools to minimize layout area and routing wirelength. Although a min-cut partitioning has a lower performance overhead, it might not hide enough wires to fully obfuscate the functionality of outsourced designs. Also, a performance-driven placement might place two connected pins/gates close-by, thereby leaking the information about the hidden connections that can be exploited by the proximity-attack algorithm, as introduced in Sect. 12.4.1.1.

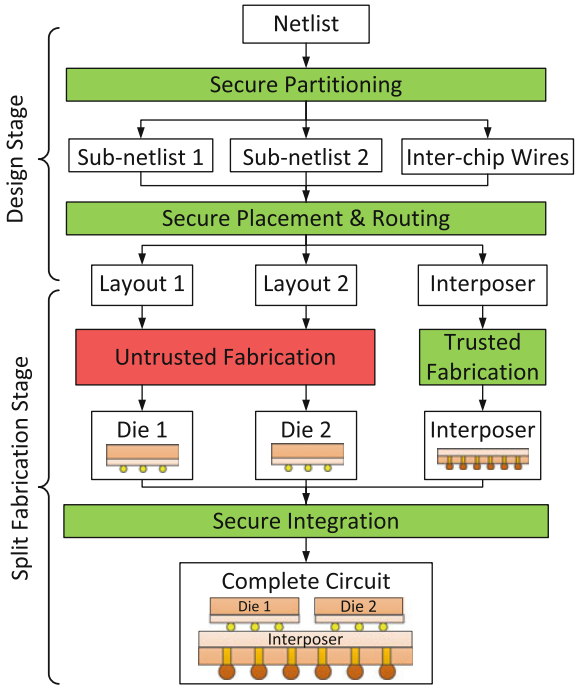

Fig. 12.4 A security-aware 2.5D IC design flow [47]

In this section, we introduce a security-aware 2.5D IC physical design flow that aims at thwarting hardware IP piracy. The security-aware 2.5D IC design and split fabrication flow of is shown in Fig. 12.4. The objective of this design flow is to thwart IP piracy by producing a security-aware partitioning and placement solution that can obfuscate the original functionality while defending the proximity attack. The *secure 2.5D design flow problem* can be defined as follows:

Given a netlist of a combinational circuit and the Boolean function F that maps its primary outputs (PO) $\mathbf{Y}$ to its primary inputs (PI) $\mathbf{X}$: $\mathbf{Y} = F(\mathbf{X})$, the objective of a security-aware 2.5D IC design flow is to find a bi-partition and a corresponding gate-level placement result, so that the placement result of two partitions will disclose the least functionality and netlist of the original circuit at a minimum performance cost.

Notice that this design and fabrication flow assumes only one untrusted offshore foundry that is responsible for fabricating two dies. However, it is possible that two dies can be outsourced to different foundries, and if these foundries are completely independent (no collusion), the information leakage to each foundry can be reduced. Moreover, this design flow focuses only on bi-partitioning for simplicity, but it would be possible to partition into more layouts and use more "independent" foundries for better security.

12.5.1 Security Metrics and Objectives

Two security metrics are utilized in order to quantify the security level of a 2.5D IC design flow, namely HD and proximity-attack correctness, as discussed in Sects. 12.4.1.1 and 12.4.1.3.

- *HD*, as defined in Eq. 12.1, is widely used to quantify the security level of functionality obfuscation [29, 30, 32]. To ensure that the functionality of a reconstructed netlist deviates substantially away from the original functionality, HD approaching 50% is desirable.
- *Proximity-attack correctness* is defined as the percentage of correct connections under proximity-attack algorithm. Attack correctness approaching 0% is desirable for a secure layout design, which indicates that the attacker cannot infer the correct connections in the trusted tier.

Based on these two security metrics, the objective of our problem can be formulated as follows:

$$\text{minimize } |HD - 50\%| + Correctness \tag{12.2}$$

A secure design flow for 2.5D IC should achieve two objectives: (a) incorrect outputs will be produced on applying incorrect connections between two partitions, i.e., the HD between the functionalities of the original netlist and the netlist reconstructed using proximity-attack algorithm is 50%; (b) the proximity-attack algorithm has 0% attack correctness.

12.5.2 Secure Partitioning

The partitioning phase plays a pivotal role in functionality obfuscation because it determines the hidden wires in interposer layer. Figure 12.5 illustrates a bi-partitioning of the c17 circuit from ISCAS85 benchmark. The cut-wires are selected as the hidden wires that will be routed in the interposer layer. The resulting cut-wires have a significant impact on the incorrectness of output logics of reconstructed netlist, because they decide whether faults can be generated and propagated to primary outputs (POs) when incorrect connections are made.

To evaluate the capability of fault occurrence and fault propagation for a cut-set, we utilize the concepts of *controllability* and *observability*. As discussed in previous chapters, controllability and observability are the two characteristics that are widely used in IC testing and security techniques. Controllability of an internal wire is the sensitivity of the wire w.r.t. the logic transition of primary inputs (PIs). It quantifies the ability of setting a wire to some values (1 or 0) through PIs in order to activate a fault (due to incorrect reconnections) inside a circuit. Observability of a wire is the sensitivity of POs w.r.t. the logic transition of the internal wire. It quantifies the ability of observing faults in POs when the logic value of a wire inside the circuit is

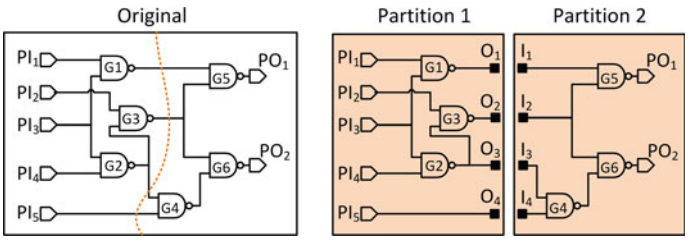

Fig. 12.5 A bi-partitioning of the c17 circuit from ISCAS85 benchmark. The cut-wires are selected as the hidden wires that will be routed in the interposer

flipped. In order to activate and produce more faults when incorrect connections are made between two partitions, we aim at selecting cut-wires with high controllability and observability. The controllability $CTRL(w)$ and observability $OBS(w)$ of a wire w can be simulated and normalized to a value between 0 to 1 [47], where 1 indicates high controllability/observability.

12.5.2.1 Secure Min-Cut Algorithm

The secure min-cut problem is to find a bi-partitioning with minimum cut-size while satisfying balance constraint and security constraint. The balance constraint ensures that two partitions have roughly equal sizes while the security constraint enforces that the controllability and observability of the wires in the cut-set are relatively large. The overall algorithm is based on Fiduccia-Mattheyses (FM) algorithm [9], a linear time heuristic approach to solve hypergraph bi-partitioning problem. The overall algorithm is as follows:

- *Initialization*: a balanced partitioning is randomly initialized so that two partitions have roughly equal sizes. PI pins and PO pins are separated into two partitions. Moreover, the controllability and observability of all wires are simulated.
- *Maintenance*: after initialization, the FM algorithm will iteratively move a gate that has the maximum cut-size drop from one block to another while maintaining the following two constraints:
  - Balance constraint: $\frac{|A(P_1)-A(P_2)|}{A(P_1)+A(P_2)} \leq B_{th}$, where $A(P_1)$, $A(P_2)$ are the sizes of two partitions P_1 and P_2, and B_{th} is a pre-defined balance threshold $0 \leq B_{th} \leq 1$.
  - Security constraint: if a gate's output wire w is in the cut-set and it has high controllability/observability $CTRL(w) + OBS(w) \geq S_{th}$, then do not move this gate. S_{th} is a pre-defined security threshold $0 \leq S_{th} \leq 2$.
- *Termination*: After all possible gate moves, the algorithm obtains a series of moves that will result in the most cut-size reduction, which produces a new partitioning solution. The algorithm is continued until it cannot find a partitioning solution with smaller cutsize. Then, a final partitioning solution is generated and each gate is assigned to a partition.

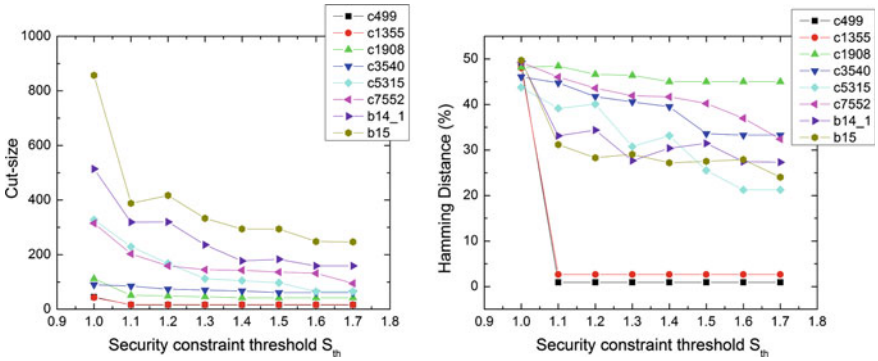

Fig. 12.6 Impact of security constraint S_{th} on **a** cut-size and **b** HD [47]

We normally run the FM algorithm multiple times with random initial partitioning solution and select the best partitioning solution with minimum cut-size as the final solution.

12.5.2.2 Trade-Off Between Cutsize and HD

In partitioning phase, we set the balance threshold B_{th} to be 0.1 to allow a slight imbalance between two partitions. Since a new security constraint is added in the secure partitioning algorithm, the feasible solution space is normally reduced. As a result, the cut-size of a partitioning solution will be increased when the security constraint is tight (S_{th} is small). The impact of S_{th} on cut-size and HD is shown in Fig. 12.6. The experiment is conducted on 8 combinational circuits from ISCAS85 and ITC99 benchmark suites. As S_{th} increases (security constraint becomes loose), the cutsize and HD decreases for all benchmarks, since a large S_{th} indicates that only few wires with large controllability and observability will be locked in the cut-set to prevent cut-size reduction. Based on this simulation results, we define **secure partitioning (SecPart)** as the partitioning with S_{th} that makes HD larger than a predefined threshold (eg 40%). Also, we define **normal partitioning (NormPart)** as the partitioning that does not consider the security constraint.

Table 12.2 shows the partitioning results of three partitioning settings, namely normal partitioning (NormPart), secure partitioning (SecPart) and normal partitioning with cut-size lower-bound that is set to the cut-size of secure partitioning solution (NormPart_LargeSize). Comparing NormPart and SecPart, we can see that HD increases from 13.24 to 46.35% on average. This is because that we have enforced the security constraint to select enough cut-wires with high controllability/observability so that more faults will be produced for an incorrectly reconstructed netlist. However, the security constraint inevitably increases the cut-size of secure partitioning. As seen, the cut-size of SecPart is 3.4× the cut-size of NormPart on average. The extra cut-wires will increase the performance overhead such as area and wirelength

Table 12.2 Benchmark information and partitioning results of normal partitioning (NormPart), normal partitioning with large cut-size (NormPart_LargeCutsize) and secure partitioning (SecPart) [47]

Benchmark	#PIs	#POs	#Gates	NormPart		NormPart_LargeSize		SecPart	
				Cutsize	HD (%)	Cutsize	HD (%)	Cutsize	HD (%)
c499	41	32	202	16	0.86	45	48.20	45	49.84
c1355	41	32	546	16	7.08	43	45.01	43	49.96
c1908	33	25	880	35	20.09	37	33.46	37	44.79
c3540	50	22	1669	57	32.82	74	33.28	74	42.67
c5315	178	123	2307	30	8.65	168	19.13	168	41.07
c7552	207	108	3512	25	5.46	155	14.34	155	48.55
b14_1	277	299	4048	99	14.85	386	19.14	386	44.76
b15	485	519	7022	168	16.14	625	27.76	625	49.12
Average	–	–	–	–	13.24	–	30.04	–	46.35

in the placement phase. To validate the efficiency of the security constraint, we compare the partitioning results of SecPart and NormPart_LargeSize. It can be seen that although these two cases have the same cut-size, SecPart can ensure 46.35% HD while NormPart_LargeSize can only achieve 30.04% HD. Therefore, with security constraint, the secure partitioning algorithm can achieve 50% HD more efficiently.

12.5.3 Secure Placement

The placement phase is designed to thwart the proximity attack by obfuscating the layouts of the untrusted tier so as to mislead the proximity-attack algorithm into making wrong connections. The goal of secure placement is to minimize the area, intra-chip wirelength, inter-chip wirelength and proximity-attack correctness.

12.5.3.1 Secure Placement Algorithm

The secure 2.5D IC placement algorithm is based on a B*-tree and simulated annealing (SA)-based 2.5D IC placement algorithm proposed by Ho et al. [13]. Figure 12.7 shows the overall flow of the secure placement algorithm.

The placement algorithm utilized the B*-tree to represent a compacted placement solution [6]. Two B*-trees are firstly constructed to represent the geometry relationship for all gates and I/O pins of two sub-netlists. A node in the B*-tree represents a gate or an I/O pin and each B*-tree represents a compacted placement for one sub-netlist. Using two B*-trees allows us to optimize the placement of two sub-netlists simultaneously. Three node perturbation operations are implemented in the SA process, as defined in [13]:

- *Rotation*: the rotation of a gate or I/O pin.
- *Move within a B*-tree*: the move of a gate or an I/O pin within same die.
- *Swap two nodes within a B*-tree*: the swap of two gates or I/O pin within same die.

After perturbation, two new B*-trees are formed and corresponding compact placements for two chips can be obtained. Based on the placement solution, we can calculate its area, inter-chip wirelength and intra-chip wirelength and perform the proximity attack to obtain the proximity-attack correctness.

The cost function of SA optimization is defined as:

$$\Phi = \alpha \times Area + \beta \times WL_{intra} + \gamma \times WL_{inter} + \theta \times Correctness \tag{12.3}$$

where α, β, γ and θ are user-specified weighting parameters, *Area* is the total area of two chips, WL_{intra} is the total intra-chip wirelength, WL_{inter} is the total inter-chip wirelength and *Correctness* is the proximity-attack correctness obtained by proximity-attack algorithm. Two SA processes are used to generate an effective and secure placement, as shown in Fig. 12.7. The first performance-driven ($\theta = 0$) SA process creates an initial placement that has optimized area and total wirelength. Based on this initial placement, the second security-driven ($\theta \neq 0$) SA process attempts to trade-off between performance and security.

In placement phase, in order to determine the optimal weights in cost function, we tested different setups on all benchmarks and define the setup $\alpha = 0.2$, $\beta = 0.7$, $\gamma = 0.1$, $\theta = 0$ as **normal placement (NormPlace)** since it can obtain relatively optimal results in area and total wirelength. For **secure placement (SecPlace)**, we increase θ to 0.05 and decrease γ to 0.05.

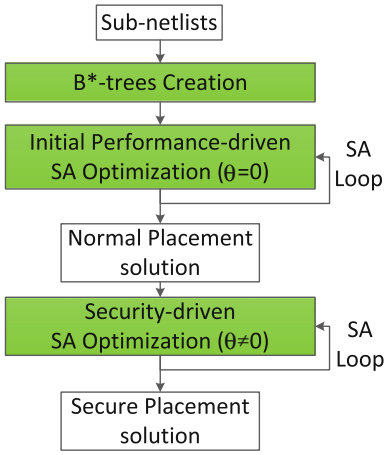

Fig. 12.7 B*-tree and SA-based secure placement algorithm flow [47]

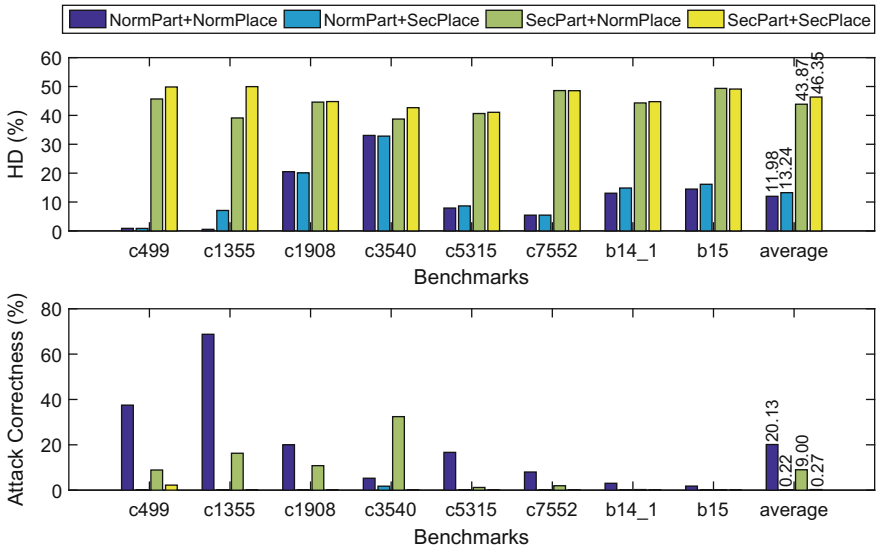

Fig. 12.8 HD and attack correctness for four design flows (NormPart + NormPlace, NormPart + SecPlace, SecPart + NormPlace, SecPart + SecPlace) [47]

12.5.4 Security and Performance Trade-Off

In order to evaluate the overall security-aware 2.5D design flow (SecPart + SecPlace), we compare four possible combinations, namely NormPart + NormPlace, NormPart + SecPlace, SecPart + NormPlace and SecPart + SecPlace in terms of attack correctness, Hamming distance, area and total wirelength.

Figure 12.8 shows the correctness and HD of proximity-attack for four cases. For 'NormPart + NormPlace', the attack correctness is 20.13%, and HD is only 11.98% because no security constraint is enforced in the NormPart to conceal the functionality, and the NormPlace does not minimize attack correctness during SA optimization. When SecPlace is performed on NormPart, we noticed that the attack correctness is limited to 0.22%, and the HD increases to 13.24%, which is still far below 50% as a large amount of functionality is exposed due to the normal min-cut partitioning. For the case 'SecPart + NormPlace', the HD increases to 43.87%, which proves the effectiveness of SecPart in concealing the functionality of a design. Finally, if we perform SecPlace on top of SecPart, compared to the 'SecPart + NormPlace' case, the attack correctness is reduced from 9.00% to 0.27% and the HD increases from 43.87% to 46.35%. The 'SecPart + SecPlace' design flow achieves the optimal security among four design flows. Overall, the SecPart algorithm is capable of approaching 50% HD, and the SecPlace algorithm can effectively achieve 0% attack correctness.

Figure 12.9 shows the area and total wirelength for four cases. Chip area and wirelength are two metrics that are commonly used to evaluate the performance of gate placement algorithm [13]. The 'NormPart+NormPlace' design flow is considered as

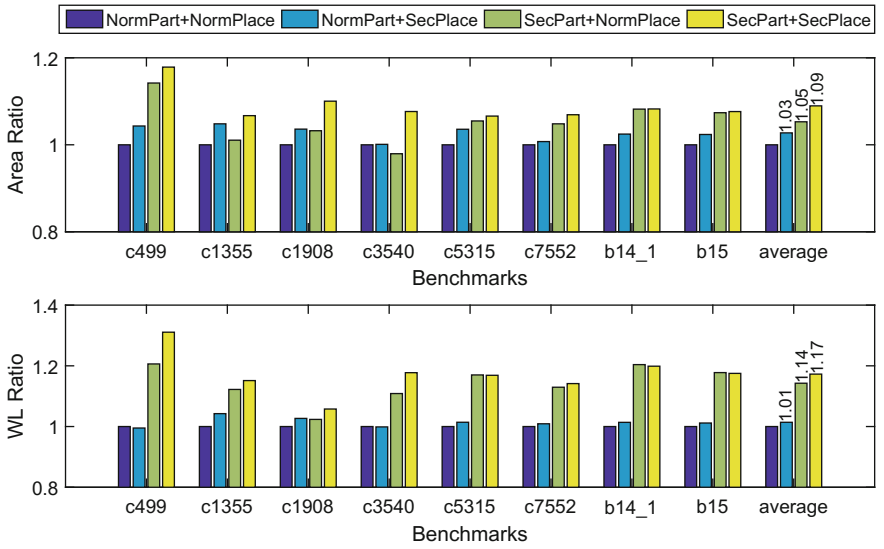

Fig. 12.9 Area and total wirelength overhead for four design flows (NormPart + NormPlace, NormPart + SecPlace, SecPart + NormPlace, SecPart + SecPlace) [47]. The NormPart + NormPlace is considered as the baseline design flow for calculating overheads, hence its overhead is 0% for all benchmarks

a baseline for calculating overheads. As seen, the main overheads come from the SecPart, as it requires a larger cut-set than NormPart to ensure 50% HD, which will inevitably increase the area and wirelength. The average overheads for SecPart are 5.29% on area and 14.27% on total wirelength. The SecPlace algorithm contributes to additional overhead because it perturbs the layout geometry to produce a placement with 0% attack correctness. Overall, the average overheads for 'SecPart+SecPlace' design flow are 8.95% on area and 17.27% on total wirelength.

12.6 Security Challenges in 3D/2.5D ICs

While providing the great promise in terms of performance and security, 3D/2.5D integration technology might also bring about adverse security impacts. In this section, we discuss various security challenges in 3D/2.5D ICs.

12.6.1 3D/2.5D IC Testing

IC testing is significant for detecting counterfeit components [12] and hardware Trojans [1, 19, 35] introduced in a global IC supply chain. The challenge of 3D IC testing stems from three aspects [24]: (1) a complicated test flow that consists of

pre-bond test, mid-bond test and post-bond test; (2) new test contents such as TSVs; (3) limited internal test accesses and mismatch between probe (50 μm) and fine-pitch micro-bumps (20 μm) for external test accesses.

Split fabrication further complicates the testing of 3D/2.5D IC. Pre-bond test performed at the untrusted foundries before die-bonding and post-bond test performed at the trusted foundry after die-bonding are both important to ensure the correctness, reliability and authenticity of an IC. However, the pre-bond test performed at the untrusted foundries might not be trustworthy. If a functional test is performed, a set of correct input–output patterns (for a die) are given to the untrusted foundries and thus there is information leakage that could help the attackers.

Emerging solutions to these challenges have been proposed. A test cost analysis has been performed to develop an economic and effective 3D test flow [37]. Redundant TSV has been proposed to reduce the yield loss due to TSV defects during fabrication [14]. Additional probe pads are integrated into each die to enable external test access and novel DfT architecture [25] for internal test access has been demonstrated. For 2.5D ICs, corresponding interposer-centric DfT architecture and post-bond testing strategy have also been proposed [7]. Moreover, secure test mechanisms such as the secure split test [8] might be employed to ensure the security of 3D/2.5D IC testing.

12.6.2 3D/2.5D IC Authentication

3D/2.5D IC is designed and fabricated by stacking/connecting multiple conventional 2D dies. How these 2D dies are connected, and how secure the dies are, will determine the vulnerability of a 3D/2.5D design. These 2D layers may contain functional IPs that are provided by third-party IP vendors and may be fabricated by different foundries. The complicated global supply chain introduces new chances for attackers to insert inauthentic (counterfeit and maliciously modified) designs to compromise the performance and security of the whole chip. Once all the layers are bonded, it is difficult to detect an inauthentic layer in the middle since the stacking structure of 3D ICs complicates physical testing and electrical testing. Thus, security-aware authentication techniques before and after bonding are of great significance. More design-for-security run-time mechanisms can also be developed to detect and/or isolate the inauthentic layers during runtime.

12.7 Implications of 3D/2.5D-Based Obfuscation on CAD Tool

While 3D/2.5D-based obfuscation offers new security opportunities to thwart various attacks, it also brings about new design challenges to the CAD tool designers since corresponding security-aware design techniques have not been well developed for the emerging technology. We summarize some of the implications on different phases of a 3D/2.5D design flow as follows:

1. *Logic Synthesis:* When 2.5D split fabrication strategy is utilized, logic synthesis poses a new impact on security [15]. Since different gate types (e.g. a NAND gate or a NOR gate) are distinguishable by their layouts, the number of gate types used in a design actually affects the difficulty of netlist obfuscation. A netlist that is synthesized using a limited number of gate types will be easier to be obfuscated using 2.5D split fabrication. However, it restricts the optimization space for logic synthesis and will result in a less optimal synthesis solution.
2. *Partitioning:* Partitioning is the core of a security-aware 3D/2.5D design flow because it determines the portion of design that is hidden from the attacker. A gate-level partitioning selects wires and/or gates into the trusted tier that can maximally obfuscate the netlist and/or functionality. Designing an optimal partitioning that can balance performance and security is challenging.
3. *Placement and Routing:* With 3D/2.5D split fabrication, a security-aware P&R algorithm is important for maintaining the secrecy of hidden portion in the trusted tier. Conventional P&R algorithm will place two connected gates/pins close-by in order to reduce wirelength. Eliminating the relationship between connectedness of two gate/pins and their physical layout proximity demands a security-aware P&R algorithm.
4. *Design Verification:* IC testing is essential to ensuring not only the correctness and reliability of an IC, but also its integrity and authenticity. 3D/2.5D integration technology complicates the testing process by introducing more layers, new contents such as TSVs while providing limited test accesses. The split fabrication strategy introduces additional complexity into the test process. The development of efficient test flow, direct test access and effective design-for-test circuitries such as build-in self-test (BIST) circuits would mitigate the testing challenge for 3D/2.5D ICs.

12.8 Summary

The stacking structure of 3D/2.5D ICs enables a new split fabrication strategy to obfuscate and protect outsourced design from supply chain attacks. A secure split fabrication-enhanced 2.5D/3D IC design flow consists of two important phases: netlist partitioning (wire and/or gate lifting) and placement. The core of the design flow is partitioning, which determines the secret information hidden from the attacker. Overall, it requires a comprehensive analysis and optimization to obtain a secure 2.5D/3D IC design flow to prevent the supply chain attacks. The true potential of 3D ICs in presence of modern security challenges has not been investigated in substantial depth. With the effort made in 3D IC security characterization and modelling, future chip designers can take security into consideration at an early phase of the design while optimizing the chip for performance and power. Moreover, novel architectures such as memory-on-chip enabled by 3D integration offer new opportunities to apply aggressive (ie high-performance overhead) security policies and mecha-

nisms to obfuscate the information flow between memory and CPU. Future 3D CPU design can incorporate security and performance advantages in 3D integration while tackling the challenges in power management, thermal dissipation and testing.

References

1. Bao C, Forte D, Srivastava A (2014) On application of one-class SVM to reverse engineering-based hardware trojan detection. In: 2014 15th International symposium on quality electronic design (ISQED). IEEE, New York, pp 47–54
2. Bao C, Forte D, Srivastava A (2015) Temperature tracking: toward robust run-time detection of hardware trojans. IEEE Trans Comput-Aided Des Integr Circuits Syst 34(10):1577–1585
3. Baumgarten A, Tyagi A, Zambreno J (2010) Preventing ic piracy using reconfigurable logic barriers. IEEE Des Test Comput 27(1):66–75
4. Bilzor M (2011) 3D execution monitor (3D-EM): using 3D circuits to detect hardware malicious inclusions in general purpose processors. In: Proceedings of the 6th international conference on information warfare and security, Academic Conferences Limited, p 288
5. Bobba S, Chakraborty A, Thomas O, Batude P, Pavlidis VF, De Micheli G (2010) Performance analysis of 3-D monolithic integrated circuits. In: IEEE international 3D systems integration conference (3DIC), 2010, IEEE, pp 1–4
6. Chang YC, Chang YW, Wu GM, Wu SW (2000) B*-trees: a new representation for non-slicing floorplans. In: Proceedings of the 37th annual design automation conference, ACM, pp 458–463
7. Chi CC, Marinissen EJ, Goel SK, Wu CW (2011) Post-bond testing of 2.5 d-sics and 3d-sics containing a passive silicon interposer base. In: IEEE international test conference (ITC), 2011, IEEE, pp 1–10
8. Contreras GK, Rahman MT, Tehranipoor M (2013) Secure split-test for preventing IC piracy by untrusted foundry and assembly. In: IEEE international symposium on defect and fault tolerance in VLSI and nanotechnology systems (DFT), 2013, IEEE, pp 196–203
9. Fiduccia CM, Mattheyses RM (1982) A linear-time heuristic for improving network partitions. In: 19th conference on design automation, 1982, IEEE, pp 175–181
10. Garrou P, Bower C, Ramm P (2011) Handbook of 3d integration: volume 1-technology and applications of 3D integrated circuits. Wiley, New York
11. Gartner Inc (2012) Market trends: Rising costs of production limit availability of leading-edge fabs. https://www.gartner.com/doc/2163515
12. Guin U, Huang K, DiMase D, Carulli JM, Tehranipoor M, Makris Y (2014) Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain. Proc IEEE 102(8):1207–1228
13. Ho YK, Chang YW (2013) Multiple chip planning for chip-interposer codesign. In: 2013 50th ACM/EDAC/IEEE design automation conference (DAC), IEEE, pp 1–6
14. Hsieh AC, Hwang T (2012) TSV redundancy: architecture and design issues in 3-D IC. IEEE Trans Very Large Scale Integr (VLSI) Sys 20(4):711–722
15. Imeson F, Emtenan A, Garg S, Tripunitara M (2013) Securing computer hardware using 3d integrated circuit (IC) technology and split manufacturing for obfuscation. In: Presented as part of the 22nd USENIX security symposium (USENIX Security 13), pp 495–510
16. Jagasivamani M, Gadfort P, Sika M, Bajura M, Fritze M (2014) Split-fabrication obfuscation: metrics and techniques. In: IEEE international symposium on hardware-oriented security and trust (HOST), 2014, IEEE, pp 7–12
17. Jung M, Song T, Wan Y, Peng Y, Lim SK (2014) On enhancing power benefits in 3d ICs: block folding and bonding styles perspective. In: Proceedings of the 51st annual design automation conference, ACM, pp 1–6

18. Khaleghi S, Da Zhao K, Rao W (2015) IC piracy prevention via design withholding and entanglement. In: The 20th Asia and south Pacific design automation conference, IEEE, pp 821–826
19. Li J, Lach J, (2008) At-speed delay characterization for IC authentication and trojan horse detection. In: IEEE international workshop on hardware-oriented security and trust (HOST), 2008, IEEE, pp 8–14
20. Liu B, Qu G (2016) VLSI supply chain security risks and mitigation techniques: a survey. Integr. VLSI J 55:438–448
21. Liu B, Wang B (2014) Embedded reconfigurable logic for asic design obfuscation against supply chain attacks. In: Proceedings of the conference on design, automation & test in Europe, European Design and Automation Association, p 243
22. Loh GH, Xie Y, Black B (2007) Processor design in 3d die-stacking technologies. IEEE Micro 27(3):31–48
23. Lu T, Srivastava A (2015) Electromigration-aware clock tree synthesis for tsv-based 3d-ics. In: Proceedings of the 25th edition on Great Lakes symposium on VLSI, ACM, pp 27–32
24. Marinissen EJ (2012) Challenges and emerging solutions in testing TSV-based 2 1/2D-and 3D-stacked ICs. In: Proceedings of the conference on design, automation and test in Europe, EDA Consortium, pp 1277–1282
25. Marinissen EJ, De Wachter B, O'Loughlin S, Deutsch S, Papameletis C, Burgherr T (2014) Vesuvius-3D: a 3D-DfT demonstrator. In: IEEE international test conference (ITC), 2014, IEEE, pp 1–10
26. Narasimhan S, Yueh W, Wang X, Mukhopadhyay S, Bhunia S (2012) Improving IC security against trojan attacks through integration of security monitors. IEEE Des Test Comput 29(5):37–46
27. Plaza SM, Markov IL (2015) Solving the third-shift problem in ic piracy with test-aware logic locking. IEEE Trans Comput-Aided Des Integr Circuits Syst 34(6):961–971
28. Rajendran J, Pino Y, Sinanoglu O, Karri R (2012) Security analysis of logic obfuscation. In: Proceedings of the 49th annual design automation conference, ACM, pp 83–89
29. Rajendran J, Sinanoglu O, Karri R (2013) Is split manufacturing secure? In: Design, automation & test in Europe conference & exhibition (DATE), 2013, IEEE, pp 1259–1264
30. Rajendran J, Sinanoglu O, Karri R (2014) Regaining trust in VLSI design: design-for-trust techniques. Proc IEEE 102(8):1266–1282
31. Rajendran J, Zhang H, Zhang C, Rose GS, Pino Y, Sinanoglu O, Karri R (2015) Fault analysis-based logic encryption. IEEE Trans Comput 64(2):410–424
32. Rostami M, Koushanfar F, Rajendran J, Karri R (2013) Hardware security: threat models and metrics. In: Proceedings of the international conference on computer-aided design, IEEE Press, pp 819–823
33. Roy JA, Koushanfar F, Markov IL (2008) Epic: ending piracy of integrated circuits. In: Proceedings of the conference on design, automation and test in Europe, ACM, pp 1069–1074
34. Saban K (2011) Xilinx stacked silicon interconnect technology delivers breakthrough FPGA capacity, bandwidth, and power efficiency. Xilinx, White Paper
35. Salmani H, Tehranipoor M, Plusquellic J, (2009) New design strategy for improving hardware trojan detection and reducing trojan activation time. In: IEEE international workshop on hardware-oriented security and trust (HOST'09), 2009, IEEE, pp 66–73
36. Subramanyan P, Ray S, Malik S (2015) Evaluating the security of logic encryption algorithms. In: IEEE international symposium on hardware oriented security and trust (HOST), 2015, IEEE, pp 137–143
37. Taouil M, Hamdioui S, Beenakker K, Marinissen EJ (2010) Test cost analysis for 3D die-to-wafer stacking. In: 19th IEEE asian test symposium (ATS), 2010, IEEE, pp 435–441
38. Tezzaron (2008) 3D-ICs and integrated circuit security. http://www.tezzaron.com/about/papers/3D-ICs_and_Integrated_Circuit_Security.pdf
39. Torrance R, James D (2009) The state-of-the-art in IC reverse engineering. In: Cryptographic hardware and embedded systems-CHES 2009, Springer, Berlin, pp 363–381

40. Vaidyanathan K, Das BP, Sumbul E, Liu R, Pileggi L (2014) Building trusted ics using split fabrication. In: IEEE international symposium on hardware-oriented security and trust (HOST), 2014, IEEE, pp 1–6
41. Vaidyanathan K, Liu R, Sumbul E, Zhu Q, Franchetti F, Pileggi L (2014) Efficient and secure intellectual property (IP) design with split fabrication. In: IEEE international symposium on hardware-oriented security and trust (HOST), 2014, IEEE, pp 13–18
42. Valamehr J, Sherwood T, Kastner R, Marangoni-Simonsen D, Huffmire T, Irvine C, Levin T (2013) A 3-D split manufacturing approach to trustworthy system development. IEEE Trans Comput-Aided Des Integr Circuits Syst 32(4):611–615
43. Wendt JB, Potkonjak M (2014) Hardware obfuscation using puf-based logic. In: Proceedings of the 2014 IEEE/ACM international conference on computer-aided design, IEEE Press, pp 270–277
44. Xiao K, Tehranipoor M (2013) BISA: Built-in self-authentication for preventing hardware trojan insertion. In: IEEE international symposium on hardware-oriented security and trust (HOST), 2013, IEEE, pp 45–50
45. Xiao K, Forte D, Tehranipoor MM (2015) Efficient and secure split manufacturing via obfuscated built-in self-authentication. In: IEEE international symposium on hardware oriented security and trust (HOST), 2015, IEEE, pp 14–19
46. Xie Y, Bao C, Serafy C, Lu T, Srivastava A, Tehranipoor M (2015) Security and vulnerability implications of 3d ics. IEEE Trans Multi-Scale Comput Syst 2(2):108–122
47. Xie Y, Bao C, Srivastava A (2015) Security-aware design flow for 2.5 d ic technology. In: Proceedings of the 5th international workshop on trustworthy embedded devices, ACM, pp 31–38
48. Yasin M, Saeed SM, Rajendran J, Sinanoglu O (2016) Activation of logic encrypted chips: Pre-test or post-test? In: 2016 design, automation & test in Europe conference & exhibition (DATE), IEEE, pp 139–144